BILLING CODE: 6750-01-P

**FEDERAL TRADE COMMISSION**

**[File No. 192 3209]**

**CafePress; Analysis of Proposed Consent Orders to Aid Public Comment**

**AGENCY:** Federal Trade Commission.

**ACTION:** Proposed consent agreement; request for comment.

**SUMMARY:** The consent agreements in this matter settle alleged violations of Federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Orders to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent orders – embodied in the consent agreements – that would settle these allegations.

**DATES:** Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

**ADDRESSES:** Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "CafePress; File No. 192 3209" on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

**FOR FURTHER INFORMATION CONTACT:** Mohammed Aijaz (214-979-9386), Federal Trade Commission Southwest Region, 1999 Bryan Street Suite 2150, Dallas, TX 75201-6808

**SUPPLEMENTARY INFORMATION:** Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreements containing consent orders to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, have been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreements and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "CafePress; File No. 192 3209" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Due to the COVID-19 pandemic and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "CafePress; File No. 192 3209" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment

does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c), 16 CFR 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC website at https://www.ftc.gov to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in

this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

**Analysis of Proposed Consent Order to Aid Public Comment**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, agreements containing consent orders from Residual Pumpkin Entity, LLC ("Residual Pumpkin") and PlanetArt, LLC ("PlanetArt") (collectively, "Respondents").

The proposed consent orders ("Proposed Orders") have been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreements and the comments received and will decide whether it should withdraw from the agreements and take appropriate action or make final the Proposed Orders.

This matter involves Respondents' data security and privacy practices. Respondent Residual Pumpkin owned CafePress until September 2020, when Residual Pumpkin sold CafePress to Respondent PlanetArt. The CafePress website allows users, known as shopkeepers, to earn commissions from sales of merchandise offered to consumers. CafePress collected information such as names, email addresses, telephone numbers and—from shopkeepers—Social Security numbers ("Personal Information"). CafePress claimed to keep this information safe, but in fact failed to provide reasonable security. For example, CafePress failed to: guard against well-known and reasonably foreseeable threats, such as SQL injection and cross-site scripting attacks; encrypt Social Security numbers; and implement a process for receiving and addressing third-party security vulnerability reports. CafePress also claimed to adhere to principles set forth in the EU-

U.S. and Swiss U.S. Privacy Shield frameworks, specifically that it would honor user requests to delete data and user choices about how email addresses would be used. Instead, CafePress failed to delete Personal Information when it was requested to do so and sent marketing emails to nearly all its consumers, even those who had not opted in to receive such messages. As a result of CafePress' data security practices, consumers' Personal Information was stolen and sold on the dark web. CafePress learned of the breach but failed to notify affected consumers. After some shopkeepers learned of the breach and closed their accounts, CafePress withheld up to $25 in payable commissions from each of those shopkeepers.

The complaint alleges that Respondents violated Section 5(a) of the FTC Act by: (1) misrepresenting the measures CafePress took to protect Personal Information; (2) misrepresenting the steps CafePress took to secure consumer accounts following security incidents; (3) failing to employ reasonable data security practices; (4) misrepresenting how CafePress would use email addresses; (5) misrepresenting CafePress's adherence to the Privacy Shield frameworks; (6) misrepresenting whether CafePress would honor deletion requests; and (7) unfairly withholding commissions payable to shopkeepers.

The Proposed Orders contain provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

*Summary of Proposed Order with Residual Pumpkin*

Part I prohibits Residual Pumpkin from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which Residual Pumpkin is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users' privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

Part II requires Residual Pumpkin to establish and implement, and thereafter maintain, a comprehensive information security program ("Security Program") that protects the privacy, security, confidentiality, and integrity of Personal Information. Part III requires Residual Pumpkin to obtain initial and biennial data security assessments for 20 years. Part IV requires Residual Pumpkin to disclose all material facts to the assessor and prohibits Residual Pumpkin from misrepresenting any fact material to the assessment required by Part II. Part V requires Residual Pumpkin to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that Residual Pumpkin has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission. Part VI requires Residual Pumpkin to notify the Commission of a "Covered Incident" within thirty days of discovering such incident.

Parts VII and VIII require Residual Pumpkin to pay to the Commission $500,000 and describe the procedures and legal rights related to that payment. Part IX requires Residual Pumpkin to provide customer information to enable the Commission to administer consumer redress. Part X requires Residual Pumpkin to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which a Residual Pumpkin has delivered a copy of the order.

Part XI requires Residual Pumpkin to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations. Part XII contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and claim substantiation, as well as all records necessary to

demonstrate compliance with the order. Part XIII contains other requirements related to the Commission's monitoring of Respondent's order compliance.

Part XIV provides the effective dates of the order, including that, with exceptions, the order will terminate in twenty (20) years.

*Summary of Proposed Order with PlanetArt*

Part I prohibits PlanetArt from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which PlanetArt is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users' privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

Part II requires PlanetArt to establish and implement, and thereafter maintain, a comprehensive information security program that protects the privacy, security, confidentiality, and integrity of Personal Information. Part III requires PlanetArt to obtain initial and biennial data security assessments for 20 years. Part IV requires PlanetArt to disclose all material facts to the assessor and prohibits PlanetArt from misrepresenting any fact material to the assessment required by Part II.

Part V requires PlanetArt to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that PlanetArt has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission. Part VI requires PlanetArt to notify the Commission of a "Covered Incident" within thirty days of discovering such incident. Parts VII requires PlanetArt to provide notice to consumers to inform them of the breach and the settlement with the FTC.

Part VIII requires PlanetArt to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which a PlanetArt has delivered a copy of the order.

Part IX requires PlanetArt to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations. Part X contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and claim substantiation, as well as all records necessary to demonstrate compliance with the order. Part XI contains other requirements related to the Commission's monitoring of PlanetArt's order compliance.

Part XII provides the effective dates of the order, including that, with exceptions, the order will terminate in 20 years.

The purpose of this analysis is to facilitate public comment on the Proposed Orders, and it is not intended to constitute an official interpretation of the complaint or Proposed Orders, or to modify the Proposed Orders' terms in any way.

By direction of the Commission.

**April J. Tabor**,

*Secretary*.

[FR Doc. 2022-06022 Filed: 3/21/2022 8:45 am; Publication Date: 3/22/2022]